Cyber Security: Malware

Team Number: 26

Team Members: Jerrel White
Caitlin Woods

Teachers: Sharee Lunsford
Karen Glennon

Sponsors: Kurtis Griess
Patty Meyer
Drew Einhorn

Areas of Science: Cyber Security

Table of Contents

Definition of Problem:

Our project is to make people more aware of a cyber attack called malware. Malware is a type of software that is created to intentionally damage, disrupt, and/or get access to a computer system when they aren't supposed to; something your computer does, that you don't want it to do. Unfortunately, not everyone is aware of malware and the many types of it. There are 5 types of Malware: Trojan (master of disguise), Unwanted Pop-ups, Virus that hides in a file and roots itself to your computer, Worm which self-replicates and Hybrid does more than one attack. We chose to investigate the Worm form of Malware because it captured our interest and how they move computer to computer.

Problem Solution:

Investigating all malware types is too large a problem to attack. Our goal, by the end of this year, was to make people more aware of the dangers of malware. We wanted to investigate how to prevent the Worm from attacking a computer. We planned to look at the effectiveness of a firewall that would prevent an attack. A firewall is a good way to stop infection of the specific worm.

When it comes to preventing unauthorized access of third parties in a private network, firewalls are used. These are the network security systems (hardware/software-based) that monitor and control the traffic flow between the Internet and private network on the basis of a set of user-defined rules. Firewalls shelter the computer network of an organization against unauthorized incoming or outgoing access and renders the best network security. There are 3 types of firewalls: packet filter, proxy server, and stateful inspection. A packet filter is a firewall that controls network access by analyzing outgoing and incoming packets to your computer. A Stateful Inspection (SPI) uses an intelligent way to ward off the unauthorized traffic by analyzing the packet headers and

inspecting the state of the packets along with providing proxy services. A Proxy Server masks your IP address and limits traffic types. We planned to investigate a packet filter firewall in our project.

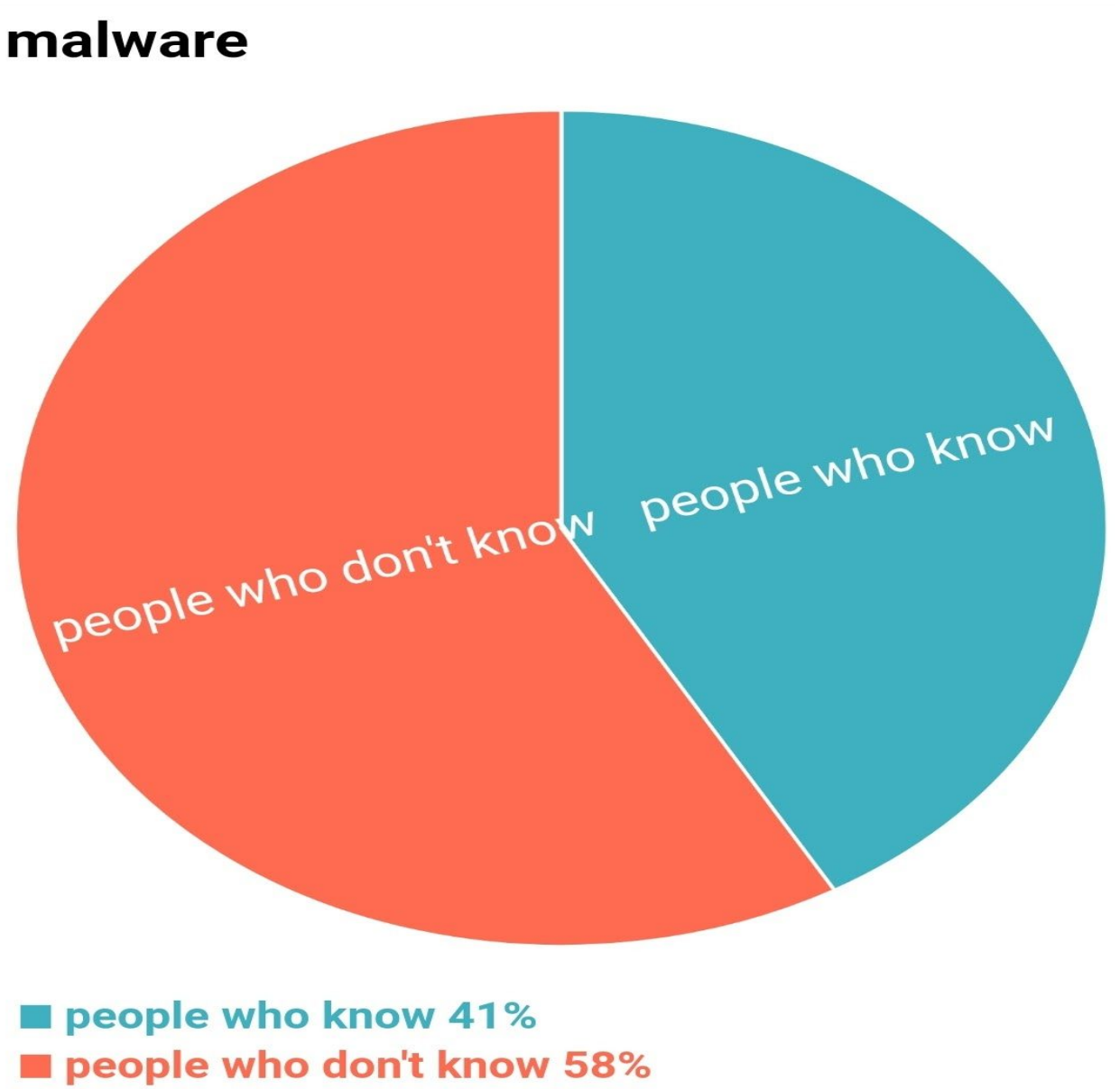
Coding:

We are coding a simulation that will show how a firewall would prevent a worm from entering our computers. We will have three firewalls going into one computer and the worm will travel through the system. We have a slider for this type of firewall. We are still working on the completion of this model.

We have created a model based off of the Wolf and Sheep Code, that is found in the NetLogo library, and also created what we imagine Malware to look like. We've interviewed Christopher Goodrich, someone who works in the cybersecurity field, and the main source for our information.

Results:

We collected data on 100 high school students by asking them if they knew what malware was. 70 percent didn't know what malware was while only 50 percent knew what malware was. Our coding was not complete when we submitted this report.


malware
people who don't know
people who know
people who know 41%
people who don't know 58%

What I have learned in this project is that even though things could be hard with doing it by yourself it's still a learning experience. My partner was not available for this report and the end of the project. Even though you might have a whole project to do as long as you have some help you can do it. I learned about malware and the different types of them and how firewalls can prevent them.

I want to thank my scientist Dave Goodrich, Drew Einhorn, Mrs. Patty, Mrs. Glennon and Ms. Lunsford.

Works Cited

1. Rhode, Matilda, et al. “Early-Stage Malware Prediction Using Recurrent Neural Networks.” *Computers & Security*, Elsevier Advanced Technology, 22 May 2018, www.sciencedirect.com/science/article/pii/S0167404818305546, What is a Computer Worm and How Does it Work?
2. How to Remove Ransomware: Virus removal steps https://www.pcrisk.com/removal-guides/16225-worm-ransomware
3. The three different types of firewalls https://bts-consulting.biz/2017/10/11/the-three-different-types-of-firewalls/
4. Jessica Rooney -NMT student
5. *The Art of Invisibility* - Mitnick, KD & Vamosi, R (2017), New York: Little, Brown and Company.