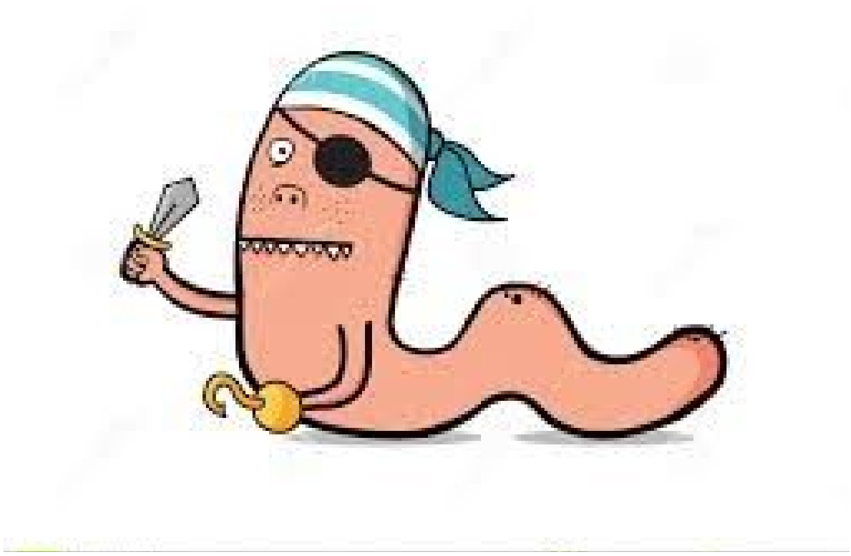
SEC-250-01
Prof. Letourneau
Due: Monday, February 22nd, 2021

Viruses & Worms



(From https://www.dreamstime.com/illustration/ugly-worm.html)

A. Creative/fun & relevant team name

The Worm Pirates

B. Names of team members

Miles Campbell, Zachary Morin, Joshua Leon Mejia, Oliver Mustoe, Alexander Brown, David Thomsen

C. Introduction & brief history of your malware type (Oliver)

Viruses and Worms are malicious files that can be both executable files and non-executable files. Viruses need to be triggered to activate, while worms do not. The idea of a virus extends back to the late 40's, but the earliest documented computer virus/worm appeared in the early 1970's, called the "creeper worm". Many famous viruses have existed throughout computer history (Michelangelo Virus, ILOVEYOU Worm, Cabir Virus) but a modern example is the "WannaCry Ransomware" which affected 150 countries and several types of businesses.

Sources:https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms, https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/#:~:text=The%20earliest%20documented%20viruses%20began,with%20being%20the%20first%20virus.&text=The%20term%20%E2%80%9Cvirus%E2%80%9D%20however%2C,introduced%20until%20the%20mid%2Deighties.

D. Tech Description:

i. What makes your malware type work? (David)

Worms can be spread through emails or other sketchy links that install the worms onto the computer and the viruses must be triggered by the activation of their host. Worms are a type of malware that spreads through multiple computers and copies itself. It is self replicating and does not need any human interference to attach to software and cause damage. Once it is installed, it is able to delete or damage files and slowly destroys the computer without the user's knowledge. https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html#:~:text=A%20computer%20worm%20is%20a,in%20order%20to%20cause%20damage.

ii. How does it infect? (Can use examples) (Miles)

There are a few ways a worm can infect a system; those include, being sent to someone as an email attachment, third party software vulnerabilities, (historically) through floppy disks, and USB flash drives. It does not require a user to click on it because it uses parts of the operating system that run automatically and are invisible to the user.

(Source 1: https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html)
(Source 2: https://searchsecurity.techtarget.com/definition/worm)

iii. How does it behave once host is infected? (Can use examples) (Zach)

A worm works by infecting other devices from the host device once the host has been compromised. They can also be designed to inject or download additional harmful software onto the computer, so the worm can effectively open the door to more attacks, like a digital battering ram. So think of it as a self-replicating digital battering ram that can eat your hard drive space without you noticing right away. Viruses on the other hand need to be activated when the computer decides to run its code.
https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

iv. How is it different from other malware types? (Josh)

The main difference between regular viruses and worms is that, worms are more of a stand alone virus that can keep propagating a network, whereas a standard virus has to be initiated by a user. Worms spread through email, the internet, downloads and FTP servers, Instant Messages, P2P/File Sharing and Networks.
https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms

E.What are some counter measures/compensating controls for your malware type?

Some counter measures you can take are by scanning the files when downloaded from the internet or your email attachment. Beware when you install the pirated software. Keep your antivirus updated and scan your system at least once a week. Possibility of a virus infection may corrupt data, so maintain your data backup. Avoid opening your email account from an unknown sender.

testing if its there using different programs such as IDA Pro

Malwarebytes IDA Pro

Counter measures: https://www.hackingloops.com/virus-worms-countermeasures/