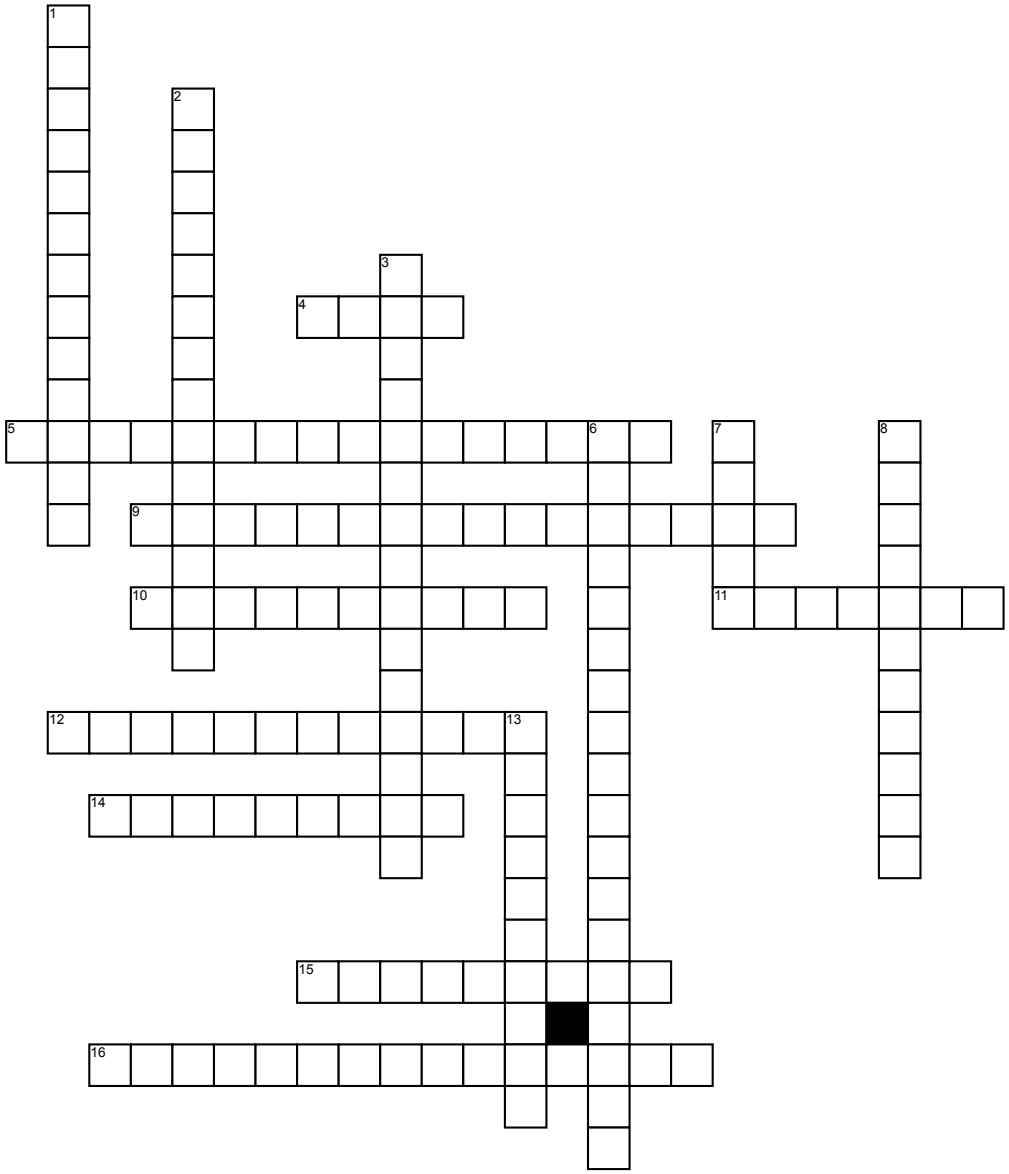
Name: _____ Date: _____

Malware



Across

4. A type of malicious software aka malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and does not need to attach itself to a software program in order to cause damage.

5. Malware that encrypts valuable files on a computer so that the user cannot access them. Cyber criminals who conduct these attacks make money by demanding that victims pay a ransom to get their files back.

9. Malware that locks the victim out of their device, preventing them from using it. Once they are locked out, cybercriminals carrying out the attack will demand a ransom to unlock the device.

10. A file-based virus that attaches to files created using programs that support macros such as Microsoft Excel and Word.

11. Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

12. This virus attaches itself to a host file and anytime you open or run the file, the virus is running. It can even overwrite the file completely.

14. A computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information.

15. Spreads through infected email messages as an attachment or a link of an infected website. Once it is installed, it will search the host computer for any email addresses contained on it. It will then start the process again, sending the malware to those email addresses without any input from the user.

16. This type of malware is designed to steal user account information for online games. The data is then transmitted to the bad actor who is controlling the Trojan.

Down

1. These are completely autonomous programs. They use an infected machine to scan the Internet for other vulnerable machines. When a vulnerable machine is located, the worm will infect it and begin the process again.

2. Used to provide the attacker with unauthorized remote access to a compromised PC system by exploiting or taking advantage of security vulnerabilities. A backdoor works in the background and hides from the user.

3. Modifies web browser settings without the user's permission and redirects the user to websites the user had not intended to visit.

6. This malware includes a backdoor for administrative control over a computer. They are usually downloaded invisibly through a user-requested program or sent as an email attachment.

7. A type of malicious program or programming code written to alter the way a computer operates and is designed to spread from one computer to another.

8. A type of malicious software aka Malware that is often disguised as legitimate software, and allows a bad actor to create a "backdoor" on a user's computer and allowing them to control it. Users are typically tricked by some form of social engineering into loading or executing a Trojan Horse on their systems.

13. A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.