**DoS–viruses, works-**

It seems there may be a misunderstanding in your question. Let me clarify the terms you mentioned: 

1. DoS (Denial-of-Service) Attacks: A DoS attack is a malicious attempt to disrupt or disable the availability of a computer system, network, or website. In a DoS attack, the attacker overwhelms the target system or network with an excessive amount of traffic, requests, or data, causing it to become unresponsive or crash. This can result in legitimate users being unable to access the targeted resource. DoS attacks can be executed using various techniques, including flooding the target with traffic (e.g., SYN flood, UDP flood) or exploiting vulnerabilities in network protocols or applications. DoS attacks aim to disrupt operations, cause inconvenience, or inflict financial losses on the target.
2. Viruses: A computer virus is a type of malicious software (malware) that infects computer systems by attaching itself to legitimate files or programs. Viruses spread by replicating and infecting other files or systems. Once activated, viruses can cause a range of harmful effects, including data corruption, unauthorized data access, system instability, or unauthorized actions by the infected system. Viruses often require human interaction, such as opening infected email attachments or executing infected files, to propagate. They can be designed to steal sensitive information, compromise system security, or cause damage to the infected system or network.
3. Worms: Worms are another form of self-replicating malware that can spread across computer networks without requiring user interaction. Unlike viruses, worms do not need to attach themselves to existing files or programs to propagate. Instead, they exploit vulnerabilities in network services or operating systems to automatically spread from one system to another. Worms can cause network congestion, degrade system performance, or install other malicious software on infected systems. Some notorious worms in the past include the Morris Worm and the Conficker worm.

It is important to note that both viruses and worms can be used in various types of cyberattacks, including DoS attacks. However, their primary functions and behaviors differ. Viruses focus on infecting files and propagating through user interactions, while worms aim to self-propagate across networks without relying on user actions.

These terms represent distinct concepts within the realm of cybersecurity, each with its own characteristics and implications.