

# Worm

It is a deceptive type of malware, designed to spread across multiple devices while remaining active on all of them. The difference between a worm and a virus is the way in which copies of themselves spread to uninfected machines. A worm is a self-sufficient malware capable of running and proliferating without user interaction - the computer does not need to be in use for the worm to activate, replicate and spread.

## How does it work?

As soon as a worm takes hold on a host machine, it can spread across a network without any help or outside action. They exploit hidden vulnerabilities in the computer's OS. Hackers create this malware to penetrate the target's OS and do their dirty work without the user's knowledge.

## What types are there?

- **By email:** Its infection vector is via email. These emails include attachments that when downloaded, executed or installed, the worm ends up accessing the recipient's device.
- **File-sharing:** File-sharing networks operate in a dubious legal manner, so hackers can easily add worms to files in high demand. These file exchanges occur mainly on peer-to-peer (P2P) networks
- **Internet:** They do not interact with their victims. Hackers use Internet or network worms to exploit vulnerabilities in an operating system.