Have you heard of multipartite viruses? Also known simply as a multi-part virus, they’ve become increasingly common in recent years. Multipartite viruses are often considered more problematic than traditional computer viruses because of their ability to spread in multiple ways. As a result, you should closely monitor your small business’s information technology (IT) for signs of a multipartite virus infection.

What Is a Multipartite Virus?

A multipartite virus is a computer virus that’s able to attack both the boot sector and executable files of an infected computer. If you’re familiar with cyber threats, you probably know that most computer viruses either attack the boot sector or executable files. Multipartite viruses, however, are unique because of their ability to attack both the boot sector and executable files simultaneously, thereby allowing them to spread in multiple ways.

According to Wikipedia, the first reported multipartite virus was identified in 1989. Known as Ghostball, it targeted the executable .com files and boot sectors of the infected computer. Being that the internet was still in its early years, Ghostball wasn’t able to reach many victims. With roughly half of the global population now connected to the internet, though, multipartite viruses pose a serious threat to businesses and consumers alike.

How Multipartite Viruses Work

Unlike with most other computer viruses, multipartite viruses are able to spread when you boot up the infected computer. The virus will typically spread through traditional methods, suck as attaching itself to executable files, but it will also spread during boot up. This characteristic is known as a “boot infector,” and it’s particularly problematic since it targets otherwise critical areas of the computer’s hard drive.

Signs of a Multipartite Virus Infection

How do you know if one or more of your small business’s computers have been infected with a multipartite virus? A telltale sign is constant pop-up messages indicating that the computer has low virtual memory. As the virus spreads to the computer’s executable files, it will automatically consume memory. And as the computer’s available, unused memory decreases, the operating system (OS) may respond with a pop-up notification.

Depending on the specific type of multipartite virus, it may automatically reformat the infected computer’s hard drive as well. This is done in an effort to overcome traditional malware protection solutions, such as anti-malware software. Even if the anti-malware software removes the infection, the multipartite virus may reformat the computer’s hard drive to reinfect it.