Nine Types of Malware

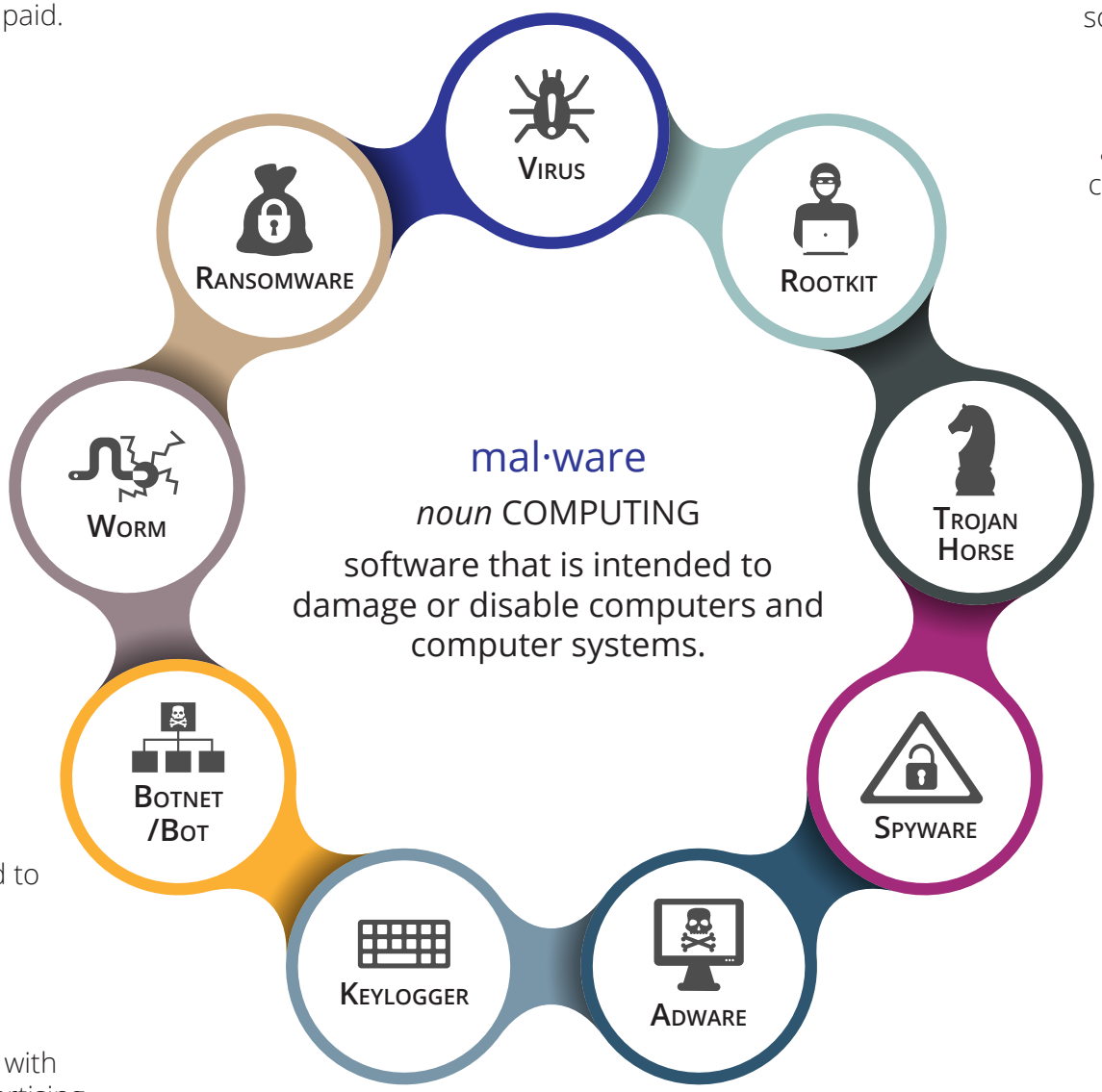
Ransomware
Software program that restricts access to a computer unless a ransom is paid.

Worm
A malicious software program that like a virus can replicate itself, but it does not rely on human action so it is very speedy in its rate of infection.

Botnet/Bot
Software robots that affect a group of computers (zombies) that are controlled by a botnet originator to create damage through activities such as distributing spam to the email contact addresses or overwhelming a server or website through a denial-of-service (DoS) attack.

Keylogger
Software that records keystrokes, which may then be uploaded to a remote server where it is analyzed to steal passwords, credit card numbers, or other private data.

Adware
Software program that may come with spyware to display unwanted advertising on your computer.



Virus
Viruses are initially contracted via software and then they can spread from one computer to another over a network or the Internet, or through removable devices, such as CDs or thumb drives. The virus could corrupt, steal, or delete data on your computer.

Rootkit
Software that gains administrator access to modify system functions and avoid detection by security measures.

Trojan Horse
As the name suggests, this is software that seems legitimate, but hides its malicious intent. It pretends to be a useful program, but when run, it can allow hackers backdoor access to computers.

Spyware
Once installed on a computer, spyware allows a hacker to monitor a user's activity, such as keystrokes, without their knowledge and may affect the user's ability to control their computer.

If you have questions about malware and how to keep your company protected call Focus Data Solutions.

FocusDataSolutions 1020 Princess Street, Alexandria, VA 22314 | 703-836-0080 | www.focusdatasolutions.com