**Virus Types and Attacks**

Understanding what a virus is, how it spreads, and the different variations is essential for defending against virus threats. You will also need to understand how a virus scanner works in order to make intelligent decisions about purchasing a virus scanner for your organisation.

**What is a Virus**

Most people are familiar with computer viruses, but may not have a clear definition of what is. A computer virus is a program that self-replicates. A virus will also have some other negative functions such as deleting files or changing system settings. However, the self-replication and rapid spread that define a virus. Often this growth, in and of itself, can be a problem for an infected network. It can lead to excessive network traffic and prevent the network from functioning properly. The more a virus floods a network with traffic, the less capacity is left for real work to be performed.

**What is a Worm**

A worm is a special type of virus. Some texts go to great lengths to differentiate worms and viruses, while others treat the worm as simply a subset of a virus. A worm is a virus that can spread without human intervention. In other words, a virus requires some human action in order to infect a machine (downloading a file, opening an attachment, and so on), but a worm can spread without such interaction. In recent years, worm eruptions have become more common than the standard, non-worm virus. Today most of what is called a “virus” is actually a worm.

**How a Virus Spreads**

The best way to combat viruses is to limit their spread, so it is critical that you understand how they spread. A virus will usually spread in one of two ways. The most common, and the simplest, method is to read your e-mail address book and e-mail itself to everyone in your address book. The second method is to simply scan your computer for connections to a network, and then copy itself to other machines on the network to which your computer has access. This is actually the most efficient way for a virus to spread, but it requires more programming skills than the other method.

The first method is, by far, the most common method for virus propagation. Microsoft Outlook may be the one e-mail program most often hit with such virus attacks. The reason is not so much a security flaw in Outlook, as it is the ease of working with Outlook.

Another way a virus can spread is by examining the affected system looking for any connected computers and copying itself to them. This sort of self-propagation does not require user interaction, so the program that uses this method to infect a system is classified as a worm.

Regardless of the way a virus arrives at your doorstep, once it is on your system, it will attempt to spread and, in many cases, will attempt to cause some harm to your system. Once a virus is on your system, it can do anything that any legitimate program can do. That means it could potentially delete files, change system settings, or cause other harm. The threat from virus attacks cannot be overstated. Some recent virus eruptions went so far as to disable existing security software, such as antivirus scanners and firewalls.

**Rombertik**

Rombertik caused chaos in 2015. This malware uses the browser to read user credentials to websites. It is sent as an attachment to an e-mail. Perhaps even worse, in some situations Rombertik will either overwrite the master boot record on the hard drive, making the machine unbootable, or begin encrypting files in the user’s home directory.

**Shamoon**

Shamoon is a computer virus discovered in 2012 designed to target computers running Microsoft Windows in the energy sector. Symantec, Kaspersky Lab, and Seculert announced its discovery on August 16, 2012. It is essentially a data-stealing program that seems to target systems in energy companies. A variant of Shamoon appeared again in 2017.

Several other viruses, worm and malware exist such as Gameover Zeus, Mirai, Linux Encoder 1, Kedi RAT and much more.

**Ransomware**

It is impossible in modern times to discuss malware and not discuss ransomware. While many people first began discussing ransomware with the advent of CrytpoLocker in 2013, ransomware has been around a lot longer than that. The first known ransomware was the 1989 PC Cyborg Trojan, which only encrypted filenames with a weak symmetric cipher. In early 2017 the WannaCry ransomware spread, starting in health care systems in the United Kingdom. It attacked unpatched Windows systems. This states the need for patching.

The Bad Rabbit computer virus spread in late 2017. This virus is ransomware. It began attacking in Russia and Ukraine, but quickly spread around the world.

**Types of Viruses**

There are many types of viruses. A virus can be classified by either its propagation method or by its activities on the target computers.

* **Macro:** Macro viruses infect the macros in office documents. Many office products, including Microsoft Office, allow users to write mini-programs called macros. These macros can also be written as a virus. A macro virus is written into a macro in some business application. For example, Microsoft Office allows users to write macros to automate some tasks. Microsoft Outlook is designed so that a programmer can write scripts using a subset of the Visual Basic programming language, called Visual Basic for Applications (VBA).  
  This scripting language is, in fact, built into all Microsoft Office products. Programmers can also use the closely related VBScript language. Both languages are quite easy to learn. If such a script is attached to an e-mail and the recipient is using Outlook, then the script can execute. That execution can do any number of things, including scanning the address book, looking for addresses, sending out e-mail, deleting e-mail, and more.
* **Boot Sector:** As the name suggests, a boot sector virus infects the boot sector of the drive, rather than the operating system. This makes them more difficult to eliminate, as most antivirus software works within the operating system.
* **Multipartite:** Multipartite viruses attack the computer in multiple ways—for example, infecting the boot sector of the hard disk and one or more files.
* **Memory resident:** A memory-resident virus installs itself and then remains in RAM from the time the computer is booted up to when it is shut down.
* **Armored:** An Armored virus uses techniques that make it hard to analyse. Code confusion is one such method. The code is written such that if the virus is disassembled, the code won’t be easily followed. Compressed code is another method for armouring the virus.
* **Stealth:** There are several types of stealth virus. A stealth virus attempts to hide itself from antivirus. A few common methods of stealth are shown below:
  + **Sparse infector:** A sparse infector virus attempts to escape detection by performing its malicious activities only sporadically. With a sparse infector virus, the user will see symptoms for a short period, then no symptoms for a time. In some cases the sparse infector targets a specific program but the virus only executes every 10th time or 20th time that target program executes. Or a sparse infector may have a burst of activity and then lie dormant for a period of time. There are a number of variations on the theme, but the basic principle is the same: to reduce the frequency of attack and thus reduce the chances for detection.
  + **Encrypted:** Sometimes a virus is encrypted, even with weak encryption, just enough to prevent an antivirus program from recognizing the virus. Then when it is time to launch an attack, the virus is decrypted.
  + **Polymorphic:** A polymorphic virus literally changes its form from time to time to avoid detection by antivirus software. A more advanced form of this is called the metamorphic virus; it can completely change itself.