ICSI MODULE 8:

Virus Types and Attacks

8.1 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.

8.1.1 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 netwo rk. It can lead to excessive network traffic and prevent the network from functioning properly. The more a virus floods a network wi th traffic, the less capacity is left for real work to be performed.

8.1.2 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 so me human action in order to infect a machine (downloading a file, opening an attachment, and so on), but a worm can spread witho ut 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.

8.1.3 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 viru s 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 Ou tlook.

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 cas es, 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 cann ot be overstated. Some recent virus eruptions went so far as to disable existing security software, such as antivirus scanners and firewalls.

8.1.3.1 Rombertik

Rombertik caused chaos in 2015. This malware uses the browser to read user credentials to websites. It is sent as an attachme nt 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.

8.3.1.2 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.

8.1.3.3 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 2103, 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. Thi s 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 qu ickly spread around the world.

8.1.4 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 targe t 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.

Virus Scanners

8.2 Virus Scanners

The most obvious defence against viruses is the virus scanner. A virus scanner is essentially software that tries to prevent a virus from infecting your system. Usually it scans incoming e-mail and other incoming traffic. Most virus scanners also have the ability to scan portable media devices such as USB drives.

In general, virus scanners work in two ways. The first method is that they contain a list of all known virus files. Generally, one of the services that vendors of virus scanners provide is a periodic update of this file. This list is typically in a small file, often called a .dat file (short for data). When you update your virus definitions, what actually occurs is that your current file is replaced by the more recent one on the vendor's website.

The antivirus program then scans your PC, network, and incoming e-mail for known virus files. Any file on your PC or attached to an e-mail is compared to the virus definition file to see whether there are any matches. With e-mail, this can be done by looking for specific subject lines and content. Known virus files often have specific phrases in the subject line and the body of the messages they are attached to. Yet viruses and worms can have a multitude of headers, some of which are very common, such as re:hello or re:thanks.

Scanning against a list of known viruses alone would result in many false positives. Therefore, the virus scanner also looks at attachments to see whether they have a certain size and creation date that matches a known virus or whether it contains known viral code. The file size, creation date, and location are the tell-tale signs of a virus. Depending on the settings of your virus scanner, you may be prompted to take some action, the file may be moved to a quarantined folder, or the file may simply be deleted outright. This type of virus scanning works only if the .dat file for the virus scanner is updated, and only for known viruses.

Another way a virus scanner can work is to monitor your system for certain types of behaviour that are typical of a virus. This might include programs that attempt to write to a hard drive's boot sector, change system files, alter the system registry, automate e-mail software, or self-multiply. Another technique virus scanners often use is searching for files that stay in memory after they execute. This is called a Terminate and Stay Resident (TSR) program. Some legitimate programs do this, but it is often a sign of a virus.

Many virus scanners have begun employing additional methods to detect viruses. Such methods include scanning system files and then monitoring any program that attempts to modify those files. This means the virus scanner must first identify specific files that are critical to the system. With a Windows system, these include the registry, the boot.ini, and possibly other files. Then, if any program attempts to alter these files, the user is warned and must first authorize the alteration before it can proceed.

It is also important to differentiate between on-demand virus scanning and ongoing scanners. An ongoing virus scanner runs in the background and is constantly checking a PC for any sign of a virus. On-demand scanners run only when you launch them. Most modern antivirus scanners offer both options.

8.2.1 Email and Attachment Scanning

Since the primary propagation method for a virus is e-mail, e-mail and attachment scanning is the most important function of any

virus scanner. Some virus scanners actually examine your e-mail on the e-mail server before downloading it to your machine. Other virus scanners work by scanning your e-mail and attachments on your computer before passing it to your e-mail program. In either case, the e-mail and its attachments should be scanned prior having any chance to open it and release the virus on your system. This is a critical difference. If the virus is first brought to your machine, and then scanned, there is a chance, however small, that the virus will still be able to infect your machine. Most commercial network virus scanners will scan the e-mail on the server before sending it on to the workstations.

8.2.2 Download Scanning

Anytime you download anything from the Internet, either via a web link or with an FTP program, there is a chance you might download an infected file. Download scanning works much like e-mail and attachment scanning, but does so on files you select for downloading.

8.2.3 File Scanning

Download and e-mail scanning will only protect your system against viruses that you might get downloading from a site, or that come to you in e-mail. Those methods will not help with viruses that are copied over a network, deposited on a shared drive, or that are already on your machine before you install the virus scanner.

This is the type of scanning in which files on your system are checked to see whether they match any known virus. This sort of scanning is generally done on an on-demand basis instead of an ongoing basis. It is a good idea to schedule your virus scanner to do a complete scan of the system periodically. I personally recommend a weekly scan, preferably at a time when no one is likely to be using the computer.

It does take time and resources to scan all the files on a computer's hard drive for infections. This type of scanning uses a method similar to e-mail and download scanning. It looks for known virus signatures. Therefore, this method is limited to finding viruses that are already known and will not find new viruses.

8.2.4 Heuristic Scanning

This is perhaps the most advanced form of virus scanning. This sort of scanning uses rules to determine whether a file or program is behaving like a virus, and is one of the best ways to find a virus that is not a known virus. A new virus will not be on any virus definition list, so you must examine its behaviour to determine whether it is a virus. However, this process is not foolproof. Some actual virus infections will be missed, and some non-virus files might be suspected of being a virus.

The unfortunate side effect of heuristic scanning is that it can easily lead to false positives. This means that it might identify a file as a virus, when in fact it is not. Most virus scanners do not simply delete viruses. They put them in a quarantined area, where you can manually examine them to determine whether you should delete the file or restore it to its original location. Examining the quarantined files rather than simply deleting them all is important because some can be false positives. In this author's personal experience, false positives are relatively rare with most modern virus scanners.

As the methods for heuristic scanning become more accurate, it is likely that more virus scanners will employ this method, and will rely on it more heavily. Such algorithms are constantly being improved. One area of research now is adding machine learning to antivirus algorithms.

8.2.5 Active Code Scanning

Modern websites frequently embed active codes, such as Java applets and ActiveX. These technologies can provide some stunning visual effects to any website. However, they can also be vehicles for malicious code. Scanning such objects before they are downloaded to your computer is an essential feature in any quality virus scanner.

8.2.6 Instant Messaging Scanning

Instant message scanning is a relatively new feature of virus scanners. Virus scanners using this technique scan instant messaging communications looking for signatures of known virus or Trojan horse files. In recent years the use of instant messaging has increased dramatically. It is now frequently used for both business and recreational purposes. This growing popularity makes virus scanning for instant messaging a vital part of effective virus scanning. If your antivirus scanner does not scan instant messaging, then you should either avoid instant messaging or select a different antivirus package.

Most commercial virus scanners use a multi-modal approach to scanning. They employ a combination of most, if not all, of the methods we have discussed here. Any scanner that does not employ most of these methods will have very little value as a security barrier for your system.

Antivirus

8.3 Antivirus

There are a number of antivirus packages available for individual computers and for network-wide virus scanning. It is important to consider the following factors when purchasing a virus scanning solution for your own organisation or recommending a solution to a client:

- **Budget:** Price should not be the only, or even the most important, consideration, but it certainly must be considered.
- **Vulnerability:** An organisation with diverse users who frequently get e-mail from outside the organisation or download from the Internet will need more antivirus protection than a small similar group that uses the Internet only occasionally.
- **Skill:** Whoever will ultimately use the product must be able to understand how to use it. Are you getting a virus scanner for a group of tech-savvy engineers or a group of end users who are unlikely to be technically proficient?
- **Technical:** How does the virus scanner work? What methods does it use to scan? How often are the .dat files updated? How quickly does the vendor respond to new virus threats and release new .dat files?

All of these factors must be considered when selecting antivirus solutions. Too often security experts simply recommend a product they are familiar with, without doing significant research.

8.3.1 McAfee

McAfee is a well-known antivirus vendor. Their antivirus has been marketed under many names, including VirusScan, Endpoint Security, and Total Protection. This company offers solutions for the home user and large organisations. All of McAfee's products have some common features, including e-mail scanning and file scanning. They also scan instant messaging traffic.

McAfee scans e-mail, files, and instant messaging for known virus signatures, and uses heuristic methods to locate new worms. Given the growing use of worms (in contrast with traditional viruses), this is an important benefit. McAfee offers a relatively easy download and install, and you can get a trial version from the company's website.

8.3.2 Norton Antivirus

Norton Antivirus is also a widely known vendor of antivirus software. You can purchase Norton solutions for individual computers or for entire networks. Norton offers e-mail and file scanning, as well as instant messaging scanning. It also offers a heuristic approach to discovering worms and traditional signature scanning. Recent versions of Norton Antivirus have also added anti-spyware and anti-adware scanning, both very useful features. An additional interesting feature of Norton Antivirus is the pre-install scan. During the installation, the install program scans the machine for any virus infections that might interfere with Norton. Because it is becoming more common to find virus attacks that actually seek to disable antivirus software, this feature is very helpful

While Norton, like most antivirus vendors, offers versions for individual PCs and for entire networks, the individual version has a free trial version you can download and experiment with for 15 days without any charge.

8.3.3 Avast Antivirus

This product is offered free for home, non-commercial uses. You can download the product from the vendor's website: www.avast.com/. You can also find professional versions, versions for Unix or Linux, and versions specifically for servers. Of particular interest is that this product is available in multiple languages including English, Dutch, Finnish, French, German, Spanish, Italian, and Hungarian.

If you download it, you can see that Avast opens up with a tutorial. This feature, combined with the fact that the home version is free, makes this a very attractive tool for the novice home user. The Multilanguage and multioperating system support make it attractive to many professionals. When it finds a virus, it sounds an alarm and then a voice states "Warning: There is a virus on your computer."

8.3.4 AVG

AVG antivirus has become quite popular. One reason is that there is a free version of it as well as a commercial version.

AVG is robust and full-featured antivirus software. It integrates with e-mail clients such as Microsoft Outlook and it also filters web traffic and downloads.

8.3.5 Kaspersky

Kaspersky has been growing in popularity. It includes business and personal versions. Like most antivirus products, it also includes additional features not directly related to detecting viruses. For example, Kaspersky includes an encrypted password vault to keep your passwords in, if you want to.

8.3.6 Panda

Panda is available in both commercial editions and free versions. The commercial version also comes with anti-spyware. Like Norton and McAfee, you can get a personal firewall bundled with the antivirus software. This product is available in English, French, and Spanish. This wide range of features makes this product a robust and effective solution.

8.3.7 Malwarebytes

This product is available from https://www.malwarebytes.com/. There is a free version of the product and a paid premium version. Malwarebytes has a strong reputation in the industry, it is well regarded, and it is rather simple to use.

8.3.8 Antivirus Policies and Procedures

Antivirus scanners are not the only facet of protecting yourself against viruses. In fact, there are situations in which a virus scanner is simply not enough. You will need policies and procedures to complete your antivirus strategy. Policies and procedures are simply written rules that dictate certain actions that administrators and end users should take and other activities they should avoid. Below are listed some policies and procedures:

- Always use a virus scanner. It costs only about $30 a year to keep your virus scanner updated. It can cost much more to not do it.
- If you are not sure about an attachment, do not open it. When you have specifically requested a file from someone, then opening an attachment from that person is probably safe. However, unexpected attachments are always cause for concern.
- Consider exchanging a code word with friends and colleagues. Tell them to put the code word in the title of the message if they wish to send you an attachment. Without the code word, do not open any attachment.
- Be sceptical of any e-mail you are sent. Keeping e-mail to official traffic will help reduce your danger. Jokes, flash movies, and so on simply should not be sent on a company e-mail system.
- Do not download files from the Internet. If you need a file downloaded, the IT department should do that, carefully scan the file, and then forward it to the user. If you feel compelled to download files you should follow two simple rules:
    - Only download from well-known, reputable sites.
    - Download to a machine that is off the network first. Then you can scan that system for viruses. In fact, if you do request your IT department to download something for you, this is likely to be the process they use.

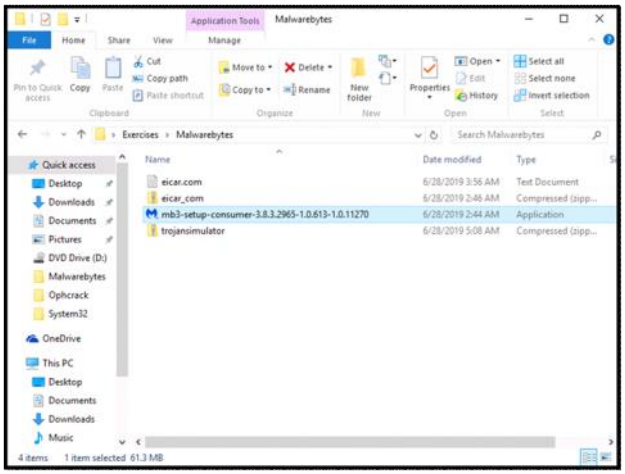
Guided Exercise: Scanning for Viruses

8.4 Guided Exercise: Scanning for Viruses

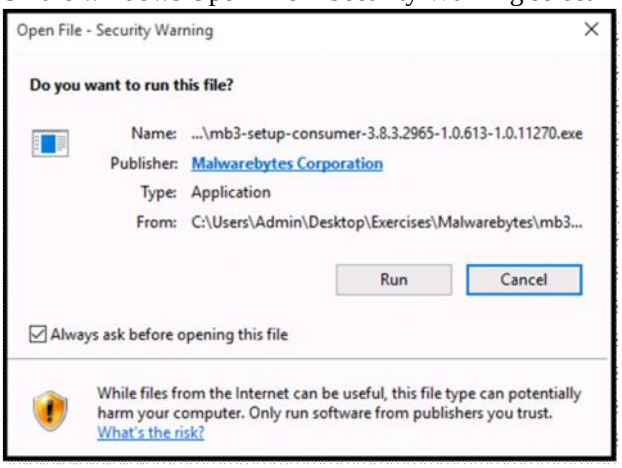
Resources	
Files	trojansimulator.zip
Machines	Windows 10

In this exercise, you are required to scan a zip file with an antivirus and identify if the file is malicious.

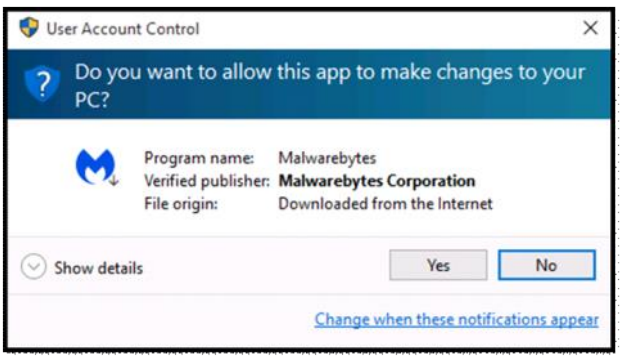
Open the desktop folder called Exercises and then the folder Malwarebytes. Double click the file mb3-setup-consumer, to install Malwarebytes.



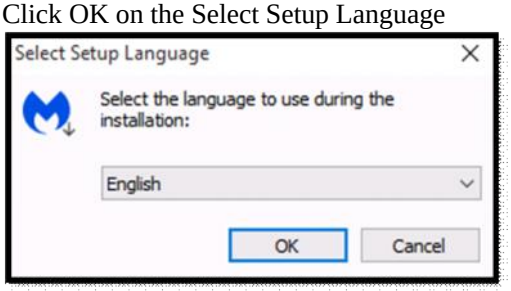
On the windows Open File – Security Warning select Run.



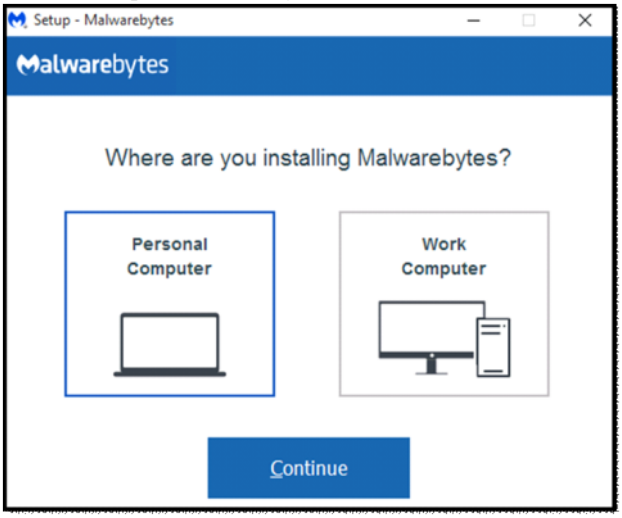
On the User Account Control windows select Yes.



Click OK on the Select Setup Language

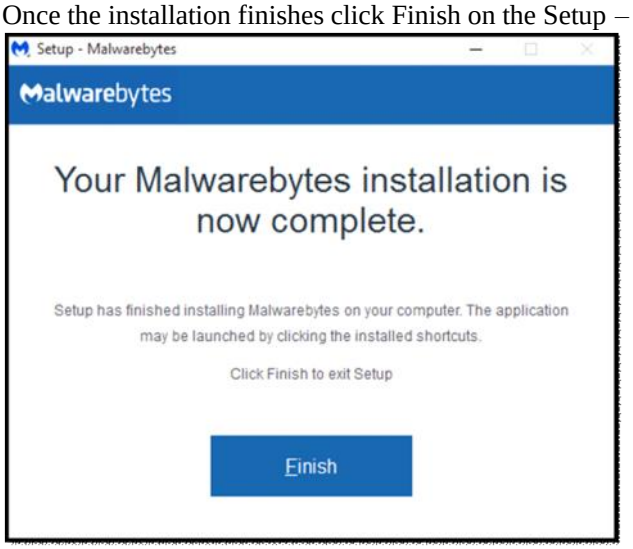


On the Setup – Malwarebytes window Select Personal computer and then click Continue

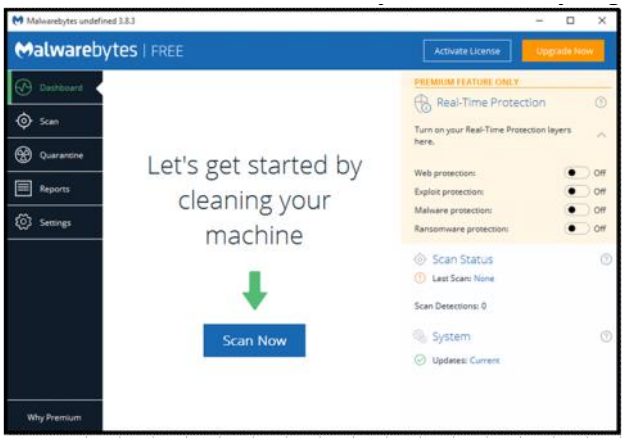


Click Agree and Continue on the Setup – Malwarebytes window.

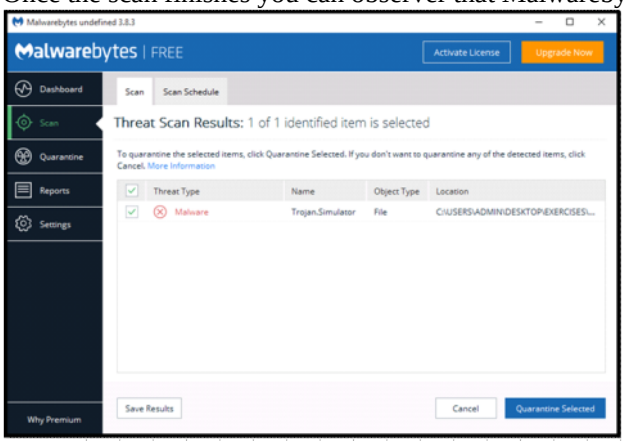
Once the installation finishes click Finish on the Setup – Malwarebytes window



Click Scan Now on the Malwarebytes window. If you get a warning for network error just ignore it after the scan finishes.



Once the scan finishes you can observer that Malwarebytes was able to identify the file trojan simulator as a malicious file.



Virus Infection and Identification

8.5 Virus Infection and Identification

The unfortunate reality is that no matter what steps you take to prevent virus infections, there is still a chance your syste m being infected with a virus. The next question is, what do you do? Some facets of your response will depend upon the severity of th e virus and how far it has spread, but generally, you need to focus on three things:

- Stopping the spread of the virus.
- Removing the virus.
- Finding out how the infection started.

8.5.1 Stopping the Spread of the Virus

In the event of a virus infection, the first priority is to stop the spread of the infection. How this is done will, depend o n how far the virus has spread. If the virus has only affected one machine, you can simply disconnect that machine from the network. Howeve r, it is unlikely that you will detect a virus before it has spread beyond a single machine. Given that fact, you will generally wi sh to follow these steps:

- If the infection is on a segment of a WAN, then immediately disconnect from that WAN connection.
- If the infection is on a subnetwork, immediately disconnect that subnetwork.
- If there are servers with sensitive data that are connected (in any way) to the infected machine (or machines), disconnect those servers. This will prevent loss of sensitive data.
- If there are backup devices connected to the infected machine or machines, disconnect them. This will prevent your backup media from becoming infected.

Obviously, your goal is to avoid getting a virus on your system. However, if that unfortunate event occur, following these st eps can minimize the damage and get your system back up and functioning in a shorter period.

8.5.2 Removing the Virus

Once you have isolated the infected machine or machines, the next step is to clean them. If you know the specific virus, then you should be able to remove it by running an antivirus program, or you should be able to find virus removal instructions on the Internet. In the highly unlikely event that you cannot remove the virus, then you may have no other choice but to format the machine (o r machines) and restore them from backups. However, it must be stressed that such a situation is very unlikely.

If you do successfully remove the virus, you will want to scan the machine thoroughly for any other virus infections before reconnecting it to your network. You should be certain it is completely clean before putting it back online.

8.5.3 Finding how the Infection Started

Once you have contained and removed the virus, the next goal is to see that it does not reappear. This is done by finding out how the virus got onto your system in the first place. To do this, you need to investigate the situation in three ways:

- Talk to users of the infected machines and see if anyone opened any e-mail attachments, downloaded anything, or installed anything. Since these are the three most likely avenues for virus infection, they should be checked first.
- Read any online documentation for that specific virus. It will tell you the normal method of propagation.
- If neither of those avenues tells you what occurred, check any activity

Trojan Horses

8.6 Trojan Horses

A Trojan horse is an application that appears to have a benign purpose but actually performs some malicious function. This deception is what makes these applications a dangerous threat to your system. The Internet is full of useful utilities (inclu ding many security tools), screen savers, images, and documents. Most Internet users do download some of these things. Creating an attr active download that has a malicious payload is an effective way of gaining access to a person's computer.

One defence against Trojan horses is to prevent all downloads, but that is not particularly practical. The value of the Inter net is the easy access it provides to such a wide variety of information—restricting that access in such a draconian manner disrupts one of the most important reasons for giving employees Internet access. Instead of using such a heavy-handed tactic, you will learn other ways to protect your systems from Trojan horses.

Once you have a Trojan horse on your system, it may perform any number of unwanted activities. Some of the most common actions Trojan horses take include:

- Erasing files on a computer.
- Spreading other malware, such as viruses. Another term for a Trojan horse that does this is a dropper.
- Using the host computer to launch distributed denial of service (DDoS) attacks or send spam.
- Searching for personal information such as bank account data.
- Installing a back door on a computer system. This means providing the creator of the Trojan horse easy access to the system, such as creating a username and password she can use to access the system.

Of the items on the above list, installing back doors and executing distributed denial of service attacks are probably the mo st frequent results of a Trojan horse attack, though installing spyware and dropping viruses are becoming much more common as we ll.

Below there is a list with some famous Trojan Horses:

- Back Orifice
- Anti-Spyware 2011
- Shedun
- Brain Test
- FinFisher
- NetBus
- FlashBack

8.6.1 Trojan Horses Symptoms

It is difficult to determine whether your system is victim of a Trojan horse. There are a number of symptoms that might indic ate that you have a Trojan horse. Assuming, of course, that you or another legitimate user are not making these changes, such symptoms include:

- Home page for your browser changing
- Any change to passwords, usernames, accounts, etc.
- Any changes to screen savers, mouse settings, backgrounds, etc.
- Any device (such as a CD door) seeming to work on its own

Any of these changes are symptoms of a Trojan horse and indicate your system is probably infected.

Spyware or Adware

8.7 Spyware or Adware

Spyware is a growing problem both for home computer users and for organisations. There is, of course, the risk that such applications might compromise some sensitive information. Another problem of such applications is that they consume too much of your system's resources. Spyware and adware both use memory. If your system has too many such applications, then they can consume so much of your system's resources that your legitimate software will have trouble running.

The primary difference between spyware and adware is what they do on your machine. They both infect your machine in the same manner. Spyware seeks to get information from your machine and make it available to some other person. This can be done in a number of ways. Adware seeks to create pop-up ads on your machine. Because these ads are not generated by the web browser, many traditional pop-up blockers will not stop them.

Both spyware and adware are growing problems for network security and home PC security. This is an important element of computer security software that was at one time largely ignored. Even today, not enough people take spyware seriously enough to guard against it. Some of these applications simply change your home page to a different site (these are known as home page hijackers); others add items to your favourites (or read items from them). Other applications can be even more intrusive.

Below there is a list with some famous spyware and adware:

- Gator
- RedSheriff

8.7.1 Anti-Spyware

Most antivirus products include anti-spyware. However, you can purchase dedicated anti-spyware software. Anti-spyware is an excellent way to defend against spyware and adware, just as antivirus software defends against viruses and Trojan horses. Essentially, it is software that scans your computer to check for spyware running on your machine. Most anti-spyware works by checking your system for known spyware files. It is difficult to identify specific activities that identify spyware, as you can with viruses. Each application must simply be checked against a list of known spyware. This means that you must maintain some sort of subscription service so that you can obtain routine updates to your spyware definition list.

In today's Internet, running anti-spyware is as essential as running antivirus software. Failing to do so can lead to serious consequences. Personal data and perhaps sensitive business data can easily leak out of your organisation without your knowledge due to spyware. You should also keep in mind that it is entirely possible for spyware to be the vehicle for purposeful industrial espionage.

QUIZ:

- 1.What is the most common method of virus propagation?
- 2.What is heuristic scanning?
- 3.Which of the below are famous Trojan Horses? (Choose two)
- 4.In the event of a virus infection, the first priority is to contact the IT department.
- 5.What malicious activity did the Rombertik virus attempt?
- 6.The unfortunate side effect of heuristic scanning is that it can easily lead to false positives
- 7.What is active code scanning?
- 8.In the context of viruses what is a .dat file?
- 9.Which of the following should be the least important consideration when purchasing antivirus software?
- 10.The first known ransomware was the 1995 PC Trojan